

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/FR05/000328

International filing date: 11 February 2005 (11.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 0401347
Filing date: 11 February 2004 (11.02.2004)

Date of receipt at the International Bureau: 15 April 2005 (15.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 22 FEV. 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr





1er dépôt

**BREVET D'INVENTION
CERTIFICAT D'UTILITÉ**

Code de la propriété intellectuelle - Livre VI



N° 11354*03

26 bis, rue de Saint Pétersbourg - 75800 Paris Cedex 08

Pour vous informer : INPI DIRECT

N° Indigo 0 825 83 85 87

0,15 € TTC/min

Télécopie : 33 (0)1 53 04 52 65

Réservé à l'INPI

REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 @ W / 030103

REMISE DES PIÈCES

DATE

11 FEV 2004

LIEU

75 INPI PARIS 34 SP

N° D'ENREGISTREMENT

0401347

NATIONAL ATTRIBUÉ PAR L'INPI

DATE DE DÉPÔT ATTRIBUÉE

PAR L'INPI

11 FEV. 2004

Vos références pour ce dossier

(facultatif) 240873 D21586 LJ

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉECabinet REGIMBEAU
20, rue de Chazelles
75847 PARIS CEDEX 17
FRANCE**Confirmation d'un dépôt par télécopie**☐ N° attribué par l'INPI à la télécopie**2** NATURE DE LA DEMANDE

Cochez l'une des 4 cases suivantes

Demande de brevet

☒

Demande de certificat d'utilité

☐

Demande divisionnaire

☐

Demande de brevet initiale

N°

Date

ou demande de certificat d'utilité initiale

N°

Date

Transformation d'une demande de

brevet européen Demande de brevet initiale

☐

N°

Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)**EMISSION DE CLE PUBLIQUE PAR TERMINAL MOBILE.****4** DÉCLARATION DE PRIORITÉ

OU REQUÊTE DU BÉNÉFICE DE

LA DATE DE DÉPÔT D'UNE

DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation

Date

N°

Pays ou organisation

Date

N°

Pays ou organisation

Date

N°

☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**5** DEMANDEUR (Cochez l'une des 2 cases)☒ Personne morale☐ Personne physiqueNom
ou dénomination sociale

FRANCE TELECOM

Prénoms

Forme juridique

SOCIETE ANONYME

N° SIREN

380129866

Code APE-NAF

Domicile

Rue

6, place d'Alleray 75015 PARIS FRANCE

ou

siège

Code postal et ville

Pays

FRANCE

Française

Nationalité

N° de téléphone (facultatif)

N° de télécopie (facultatif)

Adresse électronique (facultatif)

☐ S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»Remplir impérativement la 2^{ème} page

REMISE DES PIÈCES
DATE

11 FEV 2004

LIEU

75 INPI PARIS 34 SP

N° D'ENREGISTREMENT

0401347

NATIONAL ATTRIBUÉ PAR L'INPI

Réserve à l'INPI

DB 540 W / 030103

6 MANDATAIRE (s'il y a lieu)

240873 D21586LJ

Nom

Prénom

Cabinet ou Société

Cabinet REGIMBEAU

N° de pouvoir permanent et/ou
de lien contractuel

Adresse

Rue

20, rue de Chazelles

Code postal et ville

75847, PARIS CEDEX 17

Pays

N° de téléphone (facultatif)

01 44 29 35 00

N° de télécopie (facultatif)

01 44 29 35 99

Adresse électronique (facultatif)

info@regimbeau.fr

7 INVENTEUR (S)

Les inventeurs sont nécessairement des personnes physiques

Les demandeurs et les inventeurs
sont les mêmes personnes

☐ Oui

☒ Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)

8 RAPPORT DE RECHERCHE

Uniquement pour une demande de brevet (y compris division et transformation)

Établissement immédiat
ou établissement différé

☒

☐

Paiement échelonné de la redevance
(en deux versements)

Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt

☐ Oui

☐ Non

**9 RÉDUCTION DU TAUX
DES REDEVANCES**

Uniquement pour les personnes physiques

☐ Requête pour la première fois pour cette invention (joindre un avis de non-imposition)

☐ Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence): AG

**10 SÉQUENCES DE NUCLEOTIDES
ET/OU D'ACIDES AMINÉS**

☐ Cochez la case si la description contient une liste de séquences

Le support électronique de données est joint

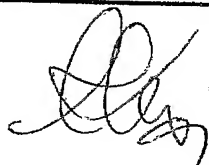
☐

La déclaration de conformité de la liste de
séquences sur support papier avec le
support électronique de données est jointe

☐

Si vous avez utilisé l'imprimé «Suite»,
indiquez le nombre de pages jointes

**11 SIGNATURE DU DEMANDEUR
OU DU MANDATAIRE
(Nom et qualité du signataire)**

 Christian
TEXIER
92-1234

VISA DE LA PRÉFECTURE
OU DE L'INPI



L'invention concerne une infrastructure à clé publique dans un
5 réseau de téléphonie mobile.

L'invention concerne également les terminaux informatiques mobiles, possédant notamment une carte SIM ou WIM.

De tels terminaux peuvent donc être des téléphones mobiles ou des téléphones WAP.

10 Ils présentent en commun la caractéristique d'avoir une carte SIM ou WIM donc d'être déjà identifié sur un réseau en rapport de l'opérateur auquel le service de téléphonie mobile a été souscrit.

Plus spécifiquement, l'invention concerne notamment une infrastructure à clé publique dans un réseau mobile.

15 Une question universelle et récurrente dans le domaine des réseaux est comment assurer la confiance entre interlocuteurs qui ne se connaissent pas et à distance. La solution existe, elle consiste à mettre en œuvre une infrastructure à clé publique (ICP ou PKI, Public Key Infrastructure).

20 Cette infrastructure possède l'avantage d'offrir aux intervenants utilisant cette infrastructure de s'appuyer sur une couche de sécurité élevée permettant l'authentification forte, la signature et le chiffrement. En revanche, elle présente l'inconvénient de son organisation qui reste complexe, longue, difficile à mettre en place et donc onéreuse pour un
25 opérateur.

De nos jours, les interactions entre les différentes entités identifiées par les certificats et l'autorité de certification sont une part importante de la gestion des certificats, c'est à dire des approbations incluant, à titre essentiel, une clé publique. Ces interactions incluent des opérations telles
30 que l'enregistrement pour la certification, le renouvellement de certificat, la révocation de certificat, la sauvegarde et le recouvrement des clés. En général, une CA (Certification Authority) doit être capable d'authentifier les identités des entités avant de répondre aux demandes. En plus les

demandes ont besoin d'être approuvées par des administrateurs autorisés ou des gestionnaires avant d'être mises en service.

Les moyens utilisés par les différentes Autorités de Certification pour vérifier une identité avant de délivrer un certificat peuvent varier largement.

5 Cela dépend notamment de l'organisation et de l'usage du certificat.

Pour se procurer plus de souplesse, les interactions avec les utilisateurs peuvent être séparées des autres fonctions de l'Autorité de Certification et gérées par un service à part appelé autorité d'enregistrement (Registration Authority ou RA).

10 Une RA agit comme une interface entre la CA en recevant les demandes des utilisateurs, les authentifiant, et les transmettant à la CA. Après réception de la réponse de la CA, la RA notifie à l'utilisateur le résultat. Les RA peuvent être utiles à l'échelle d'une PKI à travers les différents départements, sur des zones géographiques différentes ou toutes
15 autres unités dont la politique et les demandes d'authentification varient.

On peut noter ici les inconvénients de cette infrastructure : elle est longue et coûteuse à mettre en place, elle possède peu de souplesse dans la génération des certificats (liés à la politique de certification), elle a un coût important pour l'usager qui désire posséder un certificat, elle nécessite
20 une gestion importante du côté de l'opérateur de certification.

En d'autres termes, une infrastructure à clé publique offre une sécurité élevée, mais présente l'inconvénient d'une inscription préalable auprès d'une autorité d'enregistrement.

L'invention vise à rendre plus aisé le processus de certification de clé
25 publique.

Ce but est atteint selon l'invention grâce à un procédé de certification faisant appel à une autorité de certification de clé publique et faisant appel à au moins un terminal mobile apte à recevoir des messages qui soient chiffrés par cette clé publique, caractérisé en ce qu'il comporte l'étape
30 consistant à générer la clé publique au sein du terminal mobile lui-même, l'étape consistant, pour une entité de réseau de télécommunications, à acquérir cette clé auprès du terminal par une communication de réseau, et l'étape consistant, pour l'entité de réseau, à authentifier le terminal par un

processus d'authentification de l'interlocuteur utilisé dans une communication téléphonique habituelle, le procédé comprenant en outre l'étape consistant à fournir à l'autorité de certification cette clé publique en association avec le résultat de ce processus d'identification.

- 5 Un tel procédé permet notamment à un abonné à un réseau mobile, la génération d'une bi-clé par exemple puis la délivrance d'un certificat par l'opérateur.

On propose également selon l'invention un système de télécommunications mobiles, comprenant au moins un terminal mobile et
10 une entité de réseau, caractérisé en ce qu'il comporte des moyens pour générer une clé publique au sein du terminal mobile lui-même et des moyens au sein de l'entité de réseau de télécommunications pour acquérir cette clé publique auprès du terminal par une communication de réseau, ainsi que des moyens d'authentification du terminal par un processus
15 d'authentification utilisé dans une communication téléphonique habituelle, le système comprenant en outre une autorité de certification et des moyens pour fournir à l'autorité de certification la clé publique générée par le terminal mobile en association avec le résultat de ce processus d'authentification.

- 20 On propose en outre un terminal de télécommunication mobile, caractérisé en ce qu'il inclut des moyens de production d'au moins une clé destinée à déchiffrer des messages reçus par ce terminal, ainsi que des moyens pour émettre cette clé par une communication de réseau via une entité de réseau de téléphonie, à destination d'une autorité de certification
25 de sorte que celle-ci devienne une clé publique.

D'autres caractéristiques, buts et avantages de l'invention apparaîtront à la lecture de la description détaillée qui va suivre, faite en référence à la figure unique annexée, qui représente une infrastructure de certification conforme à une variante préférée de l'invention.

- 30 L'idée ici est de générer la bi-clé (clé publique et clé privée) sur le mobile de l'utilisateur puis de transmettre la clé publique à une autorité de certification par l'intermédiaire du réseau de téléphonie mobile à l'aide d'un canal sécurisé.

Cette solution décentralise les démarches et reporte la délivrance de la bi-clé dans le mobile. Cette solution allège la phase de délivrance/authentification de certificat et a un coût nul pour l'utilisateur. Pour l'opérateur, les éléments constituant cette infrastructure sont allégés.

- 5 Cette idée permet en outre de déplacer la phase d'enregistrement, cette phase étant alors aisément réalisée au moment de la souscription d'un abonnement au service de téléphonie mobile.

Elle offre l'avantage donc de pratiquement s'affranchir de cette phase.

- 10 On introduira d'abord les éléments spécifiques à l'administration actuelle des clés et des certificats. L'ensemble des moyens qui permettent l'utilisation des clés publiques et des certificats à des formats normalisés dans un environnement réseau est généralement appelé Public Key Infrastructure (PKI).

- 15 L'administration d'une PKI est un sujet complexe (gestion des clés, des certificats, listes de révocation, recouvrement...).

- Le procédé de délivrance des certificats dépend de l'autorité de certification dont ils sont issus et de leur usage. La délivrance d'un certificat doit s'effectuer selon une procédure bien définie et si l'on veut que ce
20 certificat ait une valeur, en « face à face » après, par exemple, examen de papiers d'identité.

Différentes autorités de confiance élaborent différentes politiques de délivrance de certificats.

Dans certains cas, seule l'adresse électronique suffit.

- 25 Dans d'autres cas, le login UNIX ou Windows et un mot de passe sera suffisant.

- A l'opposé, pour des certificats disposant de prérogatives importantes, le procédé de délivrance peut requérir au préalable des documents notariaux, ou encore une vérification complète de l'identité en
30 « face à face ».

Selon la politique d'organisation, le procédé de délivrance des certificats peut prendre une forme complètement transparente pour

l'utilisateur (au détriment de la sécurité) ou demander la participation significative de l'utilisateur et des procédures complexes.

En général ces procédés de délivrance de certificats doivent être très souples, ainsi les organisations peuvent les adapter à leur besoin.

- 5 Avant qu'un certificat soit délivré, la clé publique qu'il contient doit être générée en correspondance d'une clé privée qui, elle, est confidentielle.

Quelquefois, il peut être utile de délivrer un certificat à une personne pour des opérations de signature et un autre certificat pour une utilisation
10 de chiffrement.

Les clés privées, qu'elles soient de signature ou de chiffrement, sont gardées sur un support physique (carte à puces, d'ongle, USB, ...), support physique qui est détenu par la personne qu'il représente, pour assurer une sécurité élevée.

- 15 Dans un objectif de recouvrement, la clé privée de chiffrement est séquestrée sur un serveur central protégé où elle pourra être retrouvée dans le cas où l'utilisateur perd sa clé par exemple.

Une clé de chiffrement spécifiquement dédiée aux communications téléphoniques est généralement produite soit en local (poste de travail ou
20 même à l'intérieur d'une carte à puce) ou de façon centrale par exemple dans un atelier de personnalisation de carte à puce.

Par exemple, la génération de clés en local assure un service maximum de non répudiation, mais implique plus de participation de l'utilisateur dans le procédé de délivrance. La souplesse de gestion des clés
25 est essentielle pour la plupart des organisations sans négliger le côté sécurité.

Comme une carte d'identité, un certificat est soumis à une période de validité. Toute tentative d'utilisation d'un certificat avant ou après sa période de validité échouera.

- 30 Donc les mécanismes pour l'administration et le renouvellement de certificats sont essentiels pour la politique de sécurité.

Un administrateur peut vouloir être averti quand un certificat expire, ainsi un procédé de renouvellement approprié peut être mis en place et

éviter tout désagrément quant à l'utilisation de certificats qui arrivent à expiration. Le procédé de renouvellement de certificat peut impliquer la réutilisation de la même paire clé publique/clé privée ou la délivrance d'une autre.

- 5 Un certificat peut être suspendu même s'il est en cours de validité, lors d'un vol par exemple.

De manière similaire, il est quelquefois nécessaire de révoquer un certificat avant sa date d'expiration. Par exemple, si un employé quitte son entreprise ou se fait voler le support de sa bi-clé.

- 10 La révocation de certificats consiste à publier une liste de révocation de certificats (Certificate Revocation List, CRL) dans un annuaire à intervalles réguliers. La vérification de cette liste fait alors partie intégrante du procédé d'authentification.

- 15 On décrira maintenant les éléments qui se trouvent habituellement mis en œuvre de manière à assurer l'identification d'un interlocuteur et la sécurité de la communication concernée, au sein d'un réseau de télécommunications, et qui sont, pour certains de ceux ci-après décrits, mis en œuvre dans le cadre de la présente variante de l'invention.

- 20 L'infrastructure d'un réseau mobile a été conçue de manière à garantir une sécurité élevée. Le système GSM a donc recours à des procédés d'authentification et de chiffrement. Afin de garantir ce niveau de sécurité élevée, le réseau authentifie le mobile de manière forte.

Le système GSM utilise quatre types d'adressage lié à l'abonné :

- 25 - l'IMSI n'est connu qu'à l'intérieur du réseau GSM ;
- le TMSI correspond à une identité temporaire utilisée pour identifier le mobile lors des interactions mobile/réseau ;
- le MSISDN correspond au numéro de téléphone de l'abonné, c'est le seul identifiant connu de l'extérieur.
- le MSRN, qui est un numéro attribué lors de l'établissement de
30 l'appel.

Après avoir rappelé les différentes dispositions de type communes dans les réseaux de communications téléphoniques, nous allons définir maintenant quelques acronymes.

L'abréviation SIM (Subscriber Identifiant Module) définit un module d'identifiant de l'abonné.

L'abréviation IMSI (International Mobile Station Identity) qualifie un identifiant unique de l'abonné (15 chiffres), stocké dans la carte SIM.

- 5 L'abréviation TMSI (Temporary Mobile Subscriber Identity) qualifie une identité propre à un VLR, identité temporaire de l'abonné dans le VLR.

L'abréviation MSISDN (Mobile Station International ISDN Number) qualifie, elle, une identité de l'abonné qui est visible dans le monde téléphonique (exp : 33 6 98 76 54 32).

- 10 Le IMEI (International Mobile Equipment Identity) est l'identité du terminal.

Le MSRN (Mobile Station Roaming Number) est l'identité nécessaire pour acheminer les appels entre le MSC passerelle vers le PSTN et le MSC courant du mobile.

- 15 Afin d'éviter toute utilisation d'un compte mobile par une personne autre que l'abonné 10, le système GSM a recours à un procédé d'authentification visant à protéger à la fois l'abonné mais aussi l'opérateur.

- Un abonné 10 désirant s'authentifier sur le réseau, le réseau via une entité de communication 20, transmet alors un nombre aléatoire appelé RAND au mobile. La carte SIM calcule la signature de RAND à l'aide de l'algorithme A3 et la clé privée Ki stockée dans la carte SIM.
- 20

Le résultat obtenu est noté SRES, puis envoyé au réseau.

- Le réseau (ici l'entité 20), pour s'assurer de l'identité de cet abonné, va faire de même, c'est à dire qu'il calcule une signature de RAND à l'aide de A3 et de la clé Ki propre à chaque abonné et stocké sur une base de données.
- 25

Si le résultat calculé en local est identique à celui réceptionné, l'abonné est authentifié, dans le cas contraire le mobile est rejeté.

- Pour réaliser cette confidentialité, on va générer ici une clé de chiffrement appelée Kc. Cette clé se construit à l'aide de la donnée aléatoire transmise par le réseau et d'une clé privée Ki propre à l'abonné 10 et stockée dans la carte SIM.
- 30

Avec ces deux paramètres une clé Kc est générée avec l'aide de l'algorithme A8. De son côté, le réseau (l'entité 20) réalise la même opération.

La clé Ki correspondant à l'abonné identifié précédemment se trouve
5 dans une base AUC (Authentication Center), et le réseau obtient avec cette clé Ki la même clé de chiffrement Kc de son côté.

L'idée est de définir un modèle de PKI allégée avec ici les objectifs suivants, qui sont ceux de diminuer le coût de gestion pour l'opérateur, c'est à dire éviter une architecture lourde et centralisée et de s'appuyer sur
10 la sécurité de l'architecture de téléphonie et en particulier sur l'identification/authentification sur laquelle repose le système.

Il est à noter que cette solution peut s'adresser à des échanges sécurisés comme par exemple dans un environnement de travail afin de préserver la confidentialité des échanges ou bien dans le cadre de
15 communications en peer-to-peer.

Comme on l'a vu précédemment, la procédure d'authentification possède des éléments de sécurité élevée. Une fois cette phase (authentification/confidentialité) terminée, l'idée est de générer dans le téléphone un bi-clé.

20 Par la suite, l'abonné 10 envoie sa clé publique à un opérateur de certification (ici l'entité 20 elle-même). Le rôle d'opérateur de certification est donc au moins tenu partiellement par l'opérateur de téléphonie mobile lui-même.

L'authentification sur le réseau GSM est de ce fait une
25 authentification forte (possession d'un élément de sécurité et d'un secret).

Cet envoi au serveur de certification 30 est réalisé dans un tunnel sécurisé.

En d'autres termes, après réception de la clé publique, l'opérateur 20 peut certifier cette clé réceptionnée, car il est certain de l'identité
30 correspondante à la clé publique présentée : non usurpation de l'identité possible sur le réseau GSM. Puis l'opérateur 20 renvoie le certificat à son propriétaire (cas où l'entité 20 est confondue avec l'autorité de certification) et/ou le dépose sur le serveur publique de certification, ici référencé 30.

Les avantages de cette solution sont énormes, notamment la procédure de certification simplifiée, l'absence ici de processus de recouvrement, et une gestion décentralisée et reportée sur le client.

L'idée est donc de générer ici la bi-clé au sein du mobile 10 avec ici
5 les principes selon lesquels le DN (distinguished name, ou identifiant unique) pour chaque possesseur de certificat est son numéro de téléphone et chaque possesseur de certificat génère sa bi-clé et obtient un certificat par envoi de sa clé publique pour certification de manière traditionnelle. Le serveur détermine automatiquement à l'aide du DN l'origine de l'appel.

10 En outre, l'authentification de l'expéditeur (l'abonné 10) est réalisée par le réseau de téléphonie (l'entité 20). L'entité de certification 30 qui génère le certificat en correspondance avec la clé reçue est certaine de l'identité certifiée dans le certificat, grâce à l'action d'identification réalisée par l'entité de téléphonie 20, et ses moyens d'identification habituels de
15 terminal mobile.

Le serveur 30 peut donc enfin générer le certificat correspondant à la clé publique reçu puis envoyer le certificat à son propriétaire.

REVENDEICATIONS

1. Procédé de certification faisant appel à une autorité de certification (30) de clé publique et faisant appel à au moins un terminal mobile (10) apte à recevoir des messages qui soient chiffrés par cette clé publique, caractérisé en ce qu'il comporte l'étape consistant à générer la clé publique au sein du terminal mobile (10) lui-même, l'étape consistant, pour une entité (20) de réseau de télécommunications, à acquérir cette clé auprès du terminal (10) par une communication de réseau, et l'étape consistant, pour l'entité de réseau, à authentifier le terminal (10) par un processus d'authentification de l'interlocuteur utilisé dans une communication téléphonique habituelle, le procédé comprenant en outre l'étape consistant à fournir à l'autorité de certification (30) cette clé publique en association avec le résultat de ce processus d'authentification.

2. Procédé selon la revendication 1, caractérisé en ce que l'étape d'authentification du mobile (10) inclut l'émission par le mobile (10) d'un résultat de calcul faisant intervenir une clé confidentielle stockée dans le mobile, et l'étape de comparaison, par l'entité de réseau (20), du résultat avec un résultat attendu, calculé également par l'entité de réseau (20) à partir de cette même clé confidentielle, une comparaison positive étant interprétée comme une identification du terminal mobile.

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend l'étape consistant, pour l'entité de réseau, à émettre à l'attention du terminal, une donnée aléatoire, l'étape de calcul par le terminal faisant intervenir également cette donnée aléatoire émise par l'entité de réseau, l'étape de calcul par l'entité de réseau faisant aussi intervenir cette donnée aléatoire en vue de ladite comparaison de résultat.

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il met en œuvre l'étape consistant à générer au sein même du terminal mobile (10), outre la clé publique, une clé confidentielle gardée en mémoire dans le mobile (10) et adaptée à déchiffrer des messages reçus et qui ont été chiffrés avec la clé publique.

5. Procédé selon la revendication 4, caractérisé en ce que le terminal est prévu pour émettre des messages et y apposer une signature d'authentification produite à l'aide de la clé confidentielle générée par lui-même précédemment.

5 6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend l'étape consistant, pour l'entité de réseau (20), à envoyer la clé publique à l'autorité de certification (30) via un canal qui est sécurisé contre des lectures non autorisées.

10 7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend l'étape consistant pour le mobile (10) à utiliser une clé d'authentification de ce mobile (10) utilisée habituellement dans ses communications téléphoniques et à générer une clé de chiffrement, puis à chiffrer des messages à l'aide de cette clé de chiffrement puis à émettre de tels messages.

15 8. Système de télécommunications mobiles, comprenant au moins un terminal mobile (10) et une entité de réseau (20), caractérisé en ce qu'il comporte des moyens pour générer une clé publique au sein du terminal mobile (10) lui-même et des moyens au sein de l'entité de réseau de télécommunications (20) pour acquérir cette clé publique auprès du
20 terminal (10) par une communication de réseau, ainsi que des moyens d'authentification du terminal par un processus d'authentification utilisé dans une communication téléphonique habituelle, le système comprenant en outre une autorité de certification et des moyens pour fournir à l'autorité de certification la clé publique générée par le terminal mobile en association
25 avec le résultat de ce processus d'authentification.

 9. Terminal de télécommunication mobile (10), caractérisé en ce qu'il inclut des moyens de production d'au moins une clé destinée à déchiffrer des messages reçus par ce terminal, ainsi que des moyens pour émettre
30 cette clé par une communication de réseau via une entité de réseau de téléphonie (20), à destination d'une autorité de certification (30) de sorte que celle-ci devienne une clé publique.

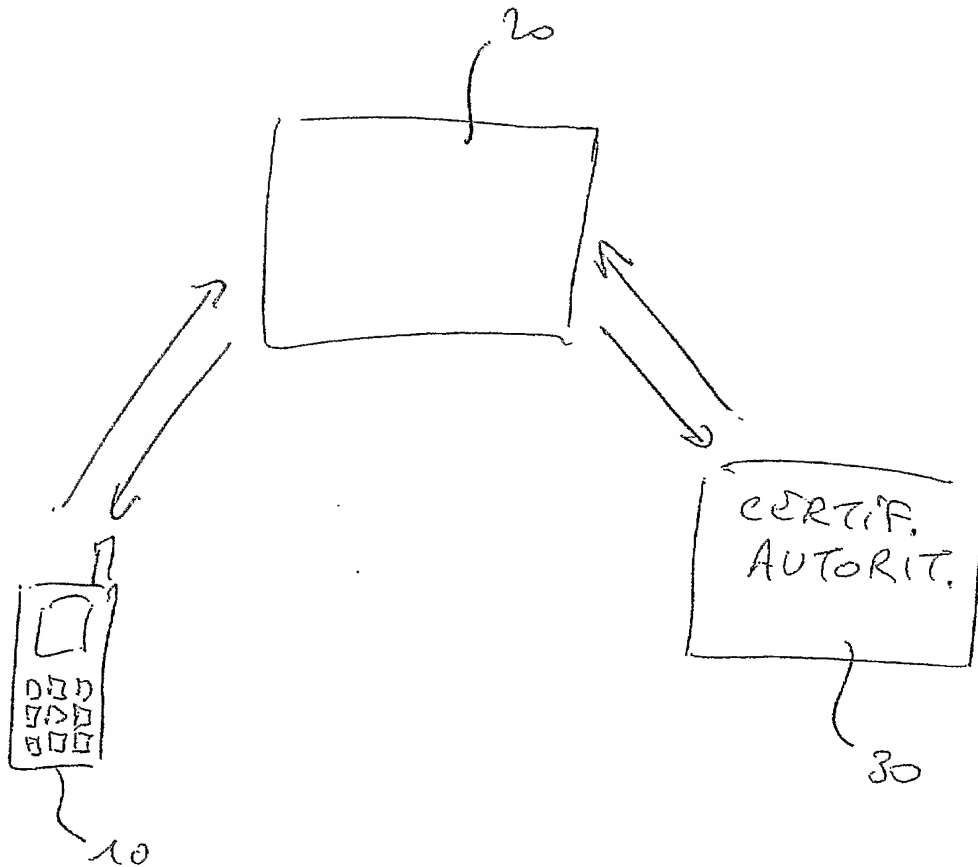
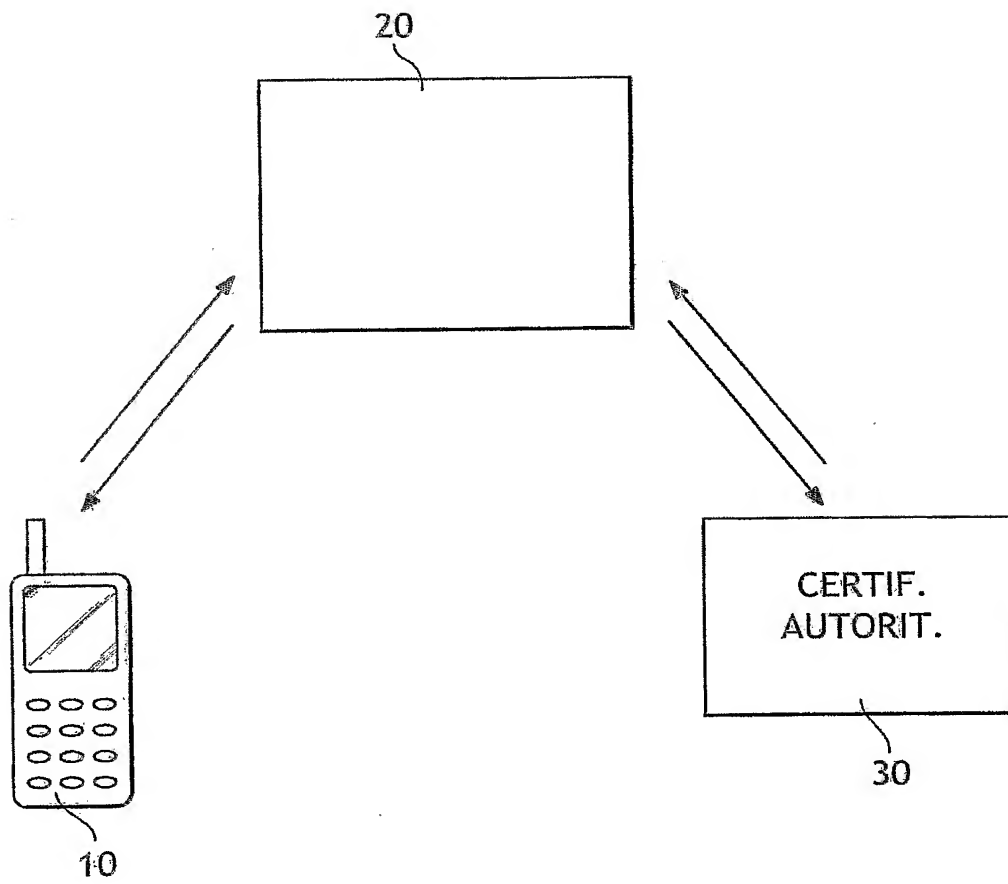


Figure unique



DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1/1...
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)



Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 300301

Vos références pour ce dossier
(facultatif)

240873 D21586 LJ

N° D'ENREGISTREMENT NATIONAL

04 01 347

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

EMISSION DE CLE PUBLIQUE PAR TERMINAL MOBILE.

LE(S) DEMANDEUR(S) :

FRANCE TELECOM :

6, place d'Alleray 75015 PARIS - FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom

Prénoms

ARDITTI David

Adresse

Rue

46ter, rue Paul Vaillant Couturier

Code postal et ville

L 92140 CLAMART FRANCE

Société d'appartenance (facultatif)

Nom

Prénoms

BEGAY Didier

Adresse

Rue

Villeneuve

Code postal et ville

L 16430 CHAMPNIERS FRANCE

Société d'appartenance (facultatif)

Nom

Prénoms

LABBE Bruno

Adresse

Rue

13, rue Gustave Courbet

Code postal et ville

L 78370 PLAISIR FRANCE

Société d'appartenance (facultatif)

DATE ET SIGNATURE(S)

DU (DES) DEMANDEUR(S)

OU DU MANDATAIRE

(Nom et qualité du signataire)

92-1284
Christian
TEXIER